UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/759,241	01/16/2004	Kristy L. Birt	END920030052US1(1397-9U)	7209

68786   7590   09/10/2008
CHRISTOPHER & WEISBERG, P.A.
200 EAST LAS OLAS BOULEVARD
SUITE 2040
FORT LAUDERDALE, FL 33301

EXAMINER
ALMEIDA, DEVIN E

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
09/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)
	10/759,241	BIRT ET AL.
	Examiner	Art Unit	
	DEVIN ALMEIDA	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>09 July 2008</u>.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5,6,8-12,16,17,19-23 and 25-30* is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5,6,8-12,16,17,19-23 and 25-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All   b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☐ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☐ Information Disclosure Statement(s) (PTO/SB/08)
  Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application
6)☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 7/09/2008

Response to arguments

Applicant's arguments have been fully considered but they are not persuasive. Kair teaches the vulnerability score is a product of a frequency score, a severity score, a criticality score and a trust score. Kair teaches F (the security vulnerability score) is computed by $F = 100 - V - E$. Where $V = \min(70, (70V_hH_h + 42V_mH_m + 14V_lH_l) / H_n))$ and $E = \min(30, \sum \text{ from } y=1 \text{ to } H_n \{R_y + W_y + 30T_y\}$. In column 64 line 20-50 Kair teaches the frequency score is based on a percentage of host experiencing the detected security vulnerability in the system. This is calculated in the V part of the security vulnerability score where H_H H_M H_L make up the number of host that have high, medium and low vulnerabilities on them. The severity score is also calculated in the V part of the security vulnerability score where high vulnerability are multiplied by 70 (root access) medium by 42 and low by 14. In column 66 lines 4-19 Kair teaches the criticality score is based on whether at least one of confidential data and personal data in on the system is calculated in the E part of the security vulnerability score. Ty part is nodes with Trojan horse that can get access to usernames passwords resources and host data on a node. The trusted score is the nodes that don't have a high medium or low vulnerability of the total nodes on the network Hn.

Claim Rejections - 35 USC § 103

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claims 1, 4-9, 12, 15-20 23, and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kair (US 7,243,148) in further view of Bellemore (5,944,825).

With respect to claim 1, 12, 23 and 25, Kair teaches the method for providing automated tracking of security vulnerabilities, comprising: using a computer device to perform a security vulnerability assessment on a system (see abstract); detecting the presence of a security vulnerability in the system; and responsive to detecting the presence of the security vulnerability (see column 13 lines 4-20); storing data obtained from the security vulnerability assessment in a security vulnerabilities database (see column 13 lines 4-20 and column 17 lines 27-38); determining using a computer program, a security vulnerability score, the security vulnerability score being a product of a frequency score, a severity score, a criticality score and a trust score (see figure 9-11, 14 and column 62 line 3 – column 66 line 19), the frequency score based on a percentage of host experiencing the detected security vulnerability in the system (see column 64 line 20-50 i.e. H_H H_M H_L), the criticality score based on whether at least one of confidential data and personal data in on the system (see column 64 lines 51-67).

Kair fails to explicitly disclose determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the determined security vulnerability score.

Bellemore discloses a method of assessing a particular host for security vulnerabilities in which he teaches determining a time to fix a security vulnerability identified by the security vulnerability assessment of the system based on the determined security vulnerability score (see Bellemore column 5, lines 16-34). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have given an allotted time for fixing the vulnerability before disabling will occur to protect the system (i.e. password disabling)(see Bellemore column 5, lines 16-34). Therefore one would have been motivated to have set a time limit for security vulnerability to be fixed to increase the security of the system

With respect to claim 5 and 16, entering an IP address associated with the security vulnerabilty and a description of the detected security vulnerability in a tracking database. (See Kair column 70 lines 28-60)

With respect to claim 6 and 17, determining delinquent security vulnerabilities based upon the determined time to fix the vulnerability detected by the security vulnerability assessment (see Bellemore column 5, lines 16-34).

With respect to claim 8 and 19, re-running a scan profile when notification is received that the security vulnerability has been fixed (See Keir column 13 lines 4-35 and column 69 lines 44-56).

With respect to claim 9 and 20, determining whether the security vulnerability still exists and archiving records associated with the security vulnerability when the security vulnerability does not exist (see Kair column 69 line 35 – column 72 line 56).

With respect to claims 27 and 29, wherein the severity score is based on whether a host will allow root compromise (see column 64 lines 51-67) and whether the security vulnerability is remotely exploitable (see column 62 line 3 – column 66 line 19).

With respect to claims 28 and 30, wherein the trust score is based on whether the system is isolated (see column 62 line 3 – column 66 line 19).

Claims 10, 11, 21, 22 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kair (US 7,243,148) in view of Bellemore (5,944,825) in further view of Dahlstrom et al (2004/0006704). With respect to claim 10, 21, 24 and 26, a method for determining a criticality factor for a security vulnerability in a computer system, comprising: Entering in a database security vulnerabilities detected in the computer system during a security vulnerability assessment (see Kair column 13 lines 4-20 and column 17 lines 27-38). Assigning a security vulnerability factor to a detected security vulnerability based upon a criticality of an element in the system, a severity of the security vulnerability with the system and isolation of the system (see Kair column 62 line 3 – column 66 line 19).

Kair does not teach measuring a frequency of occurrence for the detected security vulnerabilities and Assigning a security vulnerability factor to a detected security vulnerability based upon the frequency of occurrence of the security vulnerability in the system. Dahlstrom teaches Measuring a frequency of occurrence for the detected security vulnerabilities. (see Dahistrom paragraph 0042 and 0067). It would have been obvious at the time the invention was made to a person having

ordinary skill in the art to which said subject matter pertains to have kept track of the

frequency a security vulnerability occurs to provide an overall summaries of vulnerability

tracking within the organization or with respect to a particular product. The tracking

information may also include statistical information such as means, medians, ranges,

and deviations derived by tracking system (see paragraph 0042). Therefore one would

have been motivated to have tracked the security vulnerability.

    With respect to claim 11 and 22, wherein the criticality of an element in the

system is based on whether at least one of confidential data and personal data in on the

system and whether information on the element is used aggregation (see column 64

lines 51-67).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy

as set forth in 37 CFR 1.136(a).

    A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any

extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later

than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Devin Almeida/
Patent Examiner, GAU 2132

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132